R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

FR 00/472
EJU

REC'D 22 MAR 2000
WIPO PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 17 FEV. 2000

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Martine PLANCHE

SIEGE
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION, CERTIFICAT D'UTILITE

Code de la propriété intellectuelle-Livre VI

cerfa N° 55 -1328

REQUÊTE EN DÉLIVRANCE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 25 FEV 1999
N° D'ENREGISTREMENT NATIONAL 9902364
DÉPARTEMENT DE DÉPÔT 75 INPI PARIS
DATE DE DÉPÔT 25 FEV. 1999

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET BALLOT-SCHMIT
7 rue Le Sueur
75116 PARIS

n°du pouvoir permanent | références du correspondant | téléphone
014415 - OC/MN | 01 40 67 11 99

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ☐ certificat d'utilité ☐ transformation d'une demande de brevet européen

demande initiale ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☐ non

Titre de l'invention (200 caractères maximum)

Procédé de sécurisation d'un enchaînement d'opérations réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme

3 DEMANDEUR (S) n° SIREN . . . . . code APE-NAF . . . .

Nom et prénoms (souligner le nom patronymique) ou dénomination

STMICROELECTRONICS SA

Forme juridique

société anonyme

Nationalité (s) française

Adresse (s) complète (s)

7, avenue Galliéni
94250 GENTILLY

Pays

France

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt : joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine | numéro | date de dépôt | nature de la demande

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire)

Paul BALLOT
N° 92-1009
Cabinet BALLOT-SCHMIT

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

014415 - OC

N° D'ENREGISTREMENT NATIONAL

9902364

TITRE DE L'INVENTION :

Procédé de sécurisation d'un enchaînement d'opérations réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme

LE(S) SOUSSIGNÉ(S)

BALLOT Paul
Cabinet BALLOT-SCHMIT
7, rue Le Sueur
75116 PARIS
FRANCE

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

ROMAIN Fabrice

domicilié au :

Cabinet BALLOT-SCHMIT
7, rue Le Sueur
75116 PARIS
FRANCE

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire Paris, le 25 février 1999

BALLOT Paul
N° 92-1009
Cabinet BALLOT-SCHMIT

BA 113/140897

PROCEDE DE SECURISATION D'UN ENCHAINEMENT D'OPERATIONS REALISEES PAR UN CIRCUIT ELECTRONIQUE DANS LE CADRE DE L'EXECUTION D'UN ALGORITHME

La présente invention se rapporte à un procédé de sécurisation d'un enchaînement d'opérations réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme.

Plus particulièrement, l'invention concerne un procédé de sécurisation d'un enchaînement d'opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme, la sécurisation étant apportée par la présence d'informations parasites qui gênent l'observation, depuis l'extérieur du circuit électronique, des manifestations physiques associées à l'exécution des opérations utiles.

Dans le cadre de l'invention, un algorithme doit être compris en tant qu'enchaînement d'actions nécessaires à l'accomplissement d'une tâche. Il ne s'agit par conséquent pas nécessairement de la mise en oeuvre d'un programme informatique.

Le domaine d'application de l'invention est essentiellement le domaine de la cryptologie. La cryptologie peut se définir comme étant la science de la dissimulation de l'information. Elle constitue, avec la sécurité physique des composants et des systèmes d'exploitation, la dimension essentielle de la sécurité des cartes à puces. La cryptologie englobe la cryptographie, qui est l'art de chiffrer et de déchiffrer des messages, et la cryptanalyse, qui est l'art de casser les codes secrets.

Dans les cartes à puce, la cryptographie met en oeuvre divers mécanismes qui ont pour but d'assurer soit la confidentialité des informations, soit

l'authentification des cartes ou des utilisateurs, soit encore la signature des messages.

L'ensemble des moyens mettant en oeuvre la cryptographie forme un crypto-système. De tels crypto-systèmes renferment des informations confidentielles, notamment pour chiffrer et déchiffrer des messages numériques.

Parmi ces informations confidentielles, on peut citer les clés de chiffrement et de déchiffrement, qui sont des paramètres d'une convention secrète utilisée pour le chiffrement et le déchiffrement de messages numériques.

L'utilisation de ces clés de chiffrement et de déchiffrement nécessite souvent plusieurs transferts des données les caractérisant. Lors de leur utilisation au sein d'un crypto-système, les données caractéristiques de clés numériques et d'autres informations confidentielles circulent entre différents registres et modules de mémoire ou de traitement. Ces transferts entre registres et/ou modules se traduisent par l'apparition de courants électriques ou de champs magnétiques porteurs d'informations confidentielles. Les informations confidentielles peuvent, par exemple, concerner des clés de chiffrement et de déchiffrement.

De tels crypto-systèmes posent un problème de visibilité depuis le monde extérieur. En effet, une mesure des signaux électriques ou des champs magnétiques nés des échanges d'informations entre différentes parties du circuit peut permettre d'accéder à des informations confidentielles qui participent à la protection de données par le système de chiffrement ou de déchiffrement.

En effet, au moment de l'utilisation de la clé numérique par un composant habilité tel qu'une carte à puce, une certaine visibilité, par exemple sur la clé

numérique, est rendue possible par l'étude de tels signaux électriques. Les signaux électriques sensibles peuvent être observés sur différents bus de communication reliant différents registres ou modules de mémoire ou de traitement.

Une clé numérique peut ainsi être découverte suite à une accumulation de mesures de signaux électriques ou magnétiques et à une étude statistique de ces mesures.

D'une façon plus générale, tout circuit électronique a une consommation électrique liée aux opérations qu'il effectue. Il est possible, en mesurant cette consommation, de découvrir des informations cachées dans le circuit. Ce problème se pose en tout composant sécurisé, et notamment les composants pour cartes à puce.

La découverte de données protégées par observation de courant nécessite en général une reproductibilité de la mesure de courant afin d'effectuer les traitements statistiques.

Ainsi, lorsqu'un circuit électronique exécute un algorithme contenant des opérations identiques ou voisines, et répétitives, telles que des transferts de données confidentielles entre registres, et où l'observation fine des opérations une par une peut révéler une information confidentielle, une analyse statistique fondée sur la mesure des courants électriques précédemment cités peut nuire à la sécurité du circuit électronique.

La présente invention a pour objet de pallier les problèmes qui viennent d'être décrits.

L'invention propose donc une méthode permettant de parer à une divulgation, par observation du courant, de données protégées.

A cet effet, l'invention propose un procédé de sécurisation d'un enchaînement d'opérations réalisées

par un circuit électronique dans le cadre de l'exécution d'un algorithme qui assure la non-visibilité vis-à-vis d'une analyse des signaux électriques lors des transferts de données entre différents registres.

Pour atteindre ces objectifs, l'invention propose d'insérer des opérations factices dans un enchaînement d'opérations utiles, de même type, effectuées dans le cadre de l'exécution d'un algorithme. Les opérations factices sont très ressemblantes aux opérations utiles. Chaque opération factice est insérée à un rang aléatoire pour chaque exécution de l'algorithme. Ainsi, l'acquisition de mesures de courant comparables devient très difficile.

L'invention concerne donc un procédé de sécurisation d'un enchaînement d'opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme, chacune des opérations utiles correspondant à une étape de l'algorithme, caractérisé en ce que le procédé comprend l'étape consistant à introduire de façon aléatoire une ou plusieurs opérations factices, de même type, dans l'enchaînement d'opérations utiles.

Les différents aspects et avantages de l'invention apparaîtront plus clairement dans la suite de la description, qui présente un exemple de mise en oeuvre préféré du procédé selon l'invention et qui n'est donné qu'à titre indicatif et nullement limitatif de l'invention.

Selon un mode préféré de l'invention, un certain nombre d'opérations factices sont insérées entre des opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme. Ces opérations factices sont introduites de façon aléatoire : ces opérations factices peuvent être

introduites entre n'importe quelle opération utile associée à l'algorithme.

On peut également trouver une ou plusieurs opérations factices avant la première opération utile associée à un algorithme ou après la dernière opération utile associée à un algorithme. On peut également trouver plusieurs opérations factices consécutives.

Afin de donner des séries de mesure de courant différentes à chaque exécution d'un même algorithme, de nouveaux aléas sont introduits à chaque exécution d'un algorithme.

Néanmoins, dans une application préférée, le procédé selon l'invention comprend l'étape supplémentaire consistant à maintenir un écart de temps constant entre la réalisation de deux opérations, qu'elles soient utiles et/ou factices successives. Ainsi, l'insertion des opérations factices n'apparaît pas de façon évidente lors d'une étude temporelle des signaux électriques associés aux opérations utiles réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme.

Enfin, il est préférable, mais pas obligatoire, que le nombre d'opérations factices introduites dans l'enchaînement d'opérations utiles soit constant pour chaque nouvelle exécution de l'algorithme. Ainsi, le temps d'exécution de l'algorithme dans sa totalité est le même à chaque exécution de l'algorithme. Le fait que des opérations factices ont été introduites est ainsi invisible en première analyse, ce qui assure encore une meilleure sécurisation de l'enchaînement d'opérations utiles.

Selon l'invention, il est également possible de distribuer les aléas seulement sur certaines parties de l'algorithme. De plus, le procédé selon l'invention peut également s'appliquer à des algorithmes dont les

opérations sont ordonnées, c'est-à-dire que les opérations utiles doivent s'enchaîner dans un ordre qu'on ne peut pas changer.

Le nombre d'opérations factices introduites est, dans une application préférée de l'invention, de l'ordre de 2 pourcent sur le nombre total d'opérations effectuées.

REVENDICATIONS

1. Procédé de sécurisation d'un enchaînement d'opérations utiles, de même type, réalisées par un circuit électronique dans le cadre de l'exécution d'un algorithme, chacune des opérations utiles correspondant à une étape de l'algorithme, caractérisé en ce que le procédé comprend l'étape consistant à introduire de façon aléatoire une ou plusieurs opérations factices, de même type, dans l'enchaînement d'opérations.

2. Procédé de sécurisation d'un enchaînement d'opérations de même type selon la revendication 1, caractérisé en ce que le procédé comprend l'étape supplémentaire consistant à maintenir un écart de temps constant entre la réalisation de deux opérations utiles et/ou factices successives.

3. Procédé de sécurisation d'un enchaînement d'opérations de même type selon l'une des revendications 1 ou 2, caractérisé en ce que le nombre d'opérations factices introduites dans l'enchaînement d'opérations est constant pour chaque nouvelle exécution de l'algorithme.

4. Utilisation du procédé selon l'une des revendications précédentes dans le domaine de la cryptographie.